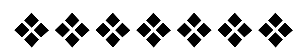
# جريمة الإرهاب الإلكتروني في ضوء أحكام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010

# The Crime of Cyberterrorism in The Light of The Arab Convention Provisions on Combating Information Technology Offences of 2010



**طالب الدكتوراه/توفيق مجاهد** *
**جامعة عبد الحميد بن باديس- مستغانم، الجزائر**
medjahed27@outlook.fr
**الدكتور/ طاهر عباسة**
**جامعة عبد الحميد بن باديس- مستغانم، الجزائر**
Taher.droit@hotmail.fr

تاريخ الاستلام: 2018/02/04 تاريخ القبول للنشر: 2018/07/24



**ملخّص:**

لقد أصبح الإرهاب الإلكتروني يشكل الهاجس الأكبر للدول، خاصة تلك التي تعمد بالدرجة الأولى على تقنية المعلومات في إدارة مصالحها الإدارية والاقتصادية والأمنية، حيث أضحت هذه التقنية سلاحا خطيرا في يد المنظمات الإرهابية تستخدمه لأغراض متعددة. وفي ظل استحالة مكافحة جرائم الفضاء الإلكتروني إلا بتعزيز جهود التعاون الأمني والقضائي والتقني بين الدول، جاءت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، لتوحيد السياسية الجنائية على المستوى الإقليمي العربي لمواجهة الجريمة الإلكترونية بما في ذلك جريمة الإرهاب الإلكتروني.

**الكلمات المفتاحية:** الإرهاب الإلكتروني؛ تقنية المعلومات؛ صور الإرهاب الإلكتروني؛ آليات مكافحة الإرهاب الإلكتروني.

***Abstract:***

*The cyberterrorism has become the biggest concern of countries, especially those which primarily rely on information technology to manage administration, economy and security services. This technology has become a dangerous weapon in the hands of terrorist organizations used for multiple purposes, In light of the impossibility of combating cybercrime, only by enhancing security, judicial and technical cooperation between different States, Arab Convention on Combating Information Technology Offences of 2010 came to unite the criminal politics at the Arab regional level to counter cybercrime, including the crime of cyberterrorism.*

**key words:** *cyberterrorism; information technology; cyberterrorism types; counter-cyberterrorism mechanisms.*

* عضو في مخبر حقوق الإنسان والحريات العامة، جامعة مستغانم.

## مقدّمــة:

إن التطور الذي شهده العالم في مجال تقنية المعلومات، ساهم بشكل كبير في التنمية الاقتصادية والاجتماعية والثقافية، بل وأصبح أكثر من ضرورة في الحياة اليومية للأفراد للتواصل فيما بينهم وتبادل الأفكار والبحث عن المعلومات والتسوق عبر الإنترنت لشراء مختلف المنتجات وتحويل الأموال...إلخ، بيد أن هذه التقنية وإن كان من الصعب حصر جميع إيجابياتها، أدت بدورها إلى ظهور العديد من الجرائم الإلكترونية العابرة للحدود التي لا يمكن لأي دولة منفردة القضاء عليها أو على الأقل الحد من انتشارها إلا بتعزيز جهود التعاون الدولي والإقليمي في المجال الأمني والقضائي والتقني.

ويعد "الإرهاب الإلكتروني" أو كما يسميه البعض "الإرهاب المعلوماتي" أو "الإرهاب السيبراني"، الذي يقابله في اللغة الفرنسية مصطلح "Le Cyberterrorisme"، من أخطر جرائم الفضاء الإلكتروني المعاصرة، التي أصبحت تشكل تهديدا حقيقيا على أمن واستقرار المجتمع الدولي برمته، نتيجةَ توظيفِ المنظماتِ الإرهابية لتقنية المعلومات، وعلى وجه الخصوص شبكة الإنترنت في تنفيذ مخططاتها الإرهابية ونشر أفكار التطرف والكراهية، والتحريض على القتل والتخريب، وتجنيد الإرهابيين، وتمويل أعمالها الإرهابية، بل والأخطر من ذلك سعي هذه المنظمات لاختراق النظم المعلوماتية للأجهزة الأمنية ومختلف المؤسسات الاقتصادية والمرافق الإدارية من أجل إتلاف أو تعديل أو تغير البيانات التي تحتويها هذه النظم أو التجسس عليها أو التحكم عن بعد في أسلحة الدمار الشامل. ويكفي في هذا المقام أن نتصور لو تمكن الإرهابيون من اختراق النظم المعلوماتية التي تتحكم في إطلاق الصواريخ النووية أو الكيماوية، فإن حجم الخسائر البشرية والمادية سيكون كارثيا في تاريخ البشرية.

وفي ظل تنامي المخاطر الأمنية والاقتصادية والفكرية والأخلاقية لجرائم البيئة الرقمية في الدول العربية، وقصور تشريعاتها الجنائية في مواجهة هذا النمط من الإجرام العابر للحدود الوطنية، وافق وزراء الداخلية ووزراء العدل العرب في اجتماعهما المشترك في 21 ديسمبر 2010 بمدينة القاهرة على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، من أجل توحيد السياسة الجنائية لحماية المجتمع العربي من خطر وآثار هذه الجرائم بما فيها جريمة الإرهاب الإلكتروني.

لدراسة هذا الموضوع والإحاطة بجميع تفاصيله، نطرح الإشكالية التالية: كيف عالجت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 جريمة الإرهاب الإلكتروني؟ وما هي الآليات التي اعتمدتها لمواجهة هذه الجريمة؟

ونظرا لأهمية هذا موضوع، وتفرع مصطلحاته الحديثة المرتبطة بالتطور المستمر في تقنية المعلومات وما يكتنفه من غموض، اعتمدنا على المنهج الوصفي التحليلي كونه أكثر ملائمة لدراسة مثل هذه المواضيع القانونية.

وانطلقنا في دراستنا من الفرضيات التالية:

- عدم وجود تعريف متفق عليه للإرهاب التقليدي، يؤدي إلى صعوبة تعريف الإرهاب الإلكتروني.
- توسيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لنطاق تجريم ظاهرة الإرهاب الإلكتروني.
- تساهم الآليات التي اعتمدتها هذه الاتفاقية، مساهمة فعالة في الحد من انتشار الإرهاب الإلكتروني.

وتهدف هذه الدراسة إلى توضيح مفهوم الإرهاب الإلكتروني، وإبراز أهم صوره، وتحديد خصائصه التي تميزه عن باقي جرائم الإرهاب الأخرى التي ترتكب في العالم المادي، وبيان نطاق تجريمه في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، والآليات التي نصت عليها لمكافحة هذه الجريمة الخطيرة.

وللإجابة على الإشكالية المطروحة، قسمنا هذه الدراسة إلى مبحثين؛ المبحث الأول سنتطرق فيه إلى مفهوم الإرهاب الإلكتروني، أما المبحث الثاني فسنتناول فيه موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من هذه الجريمة.

## المبحث الأول

## مفهوم الإرهاب الإلكتروني

يعتبر الإرهاب الإلكتروني أحد أخطر أشكال الإرهاب الدولي المعاصر، نظرا لتعدد وتنوع جرائمه وسهولة ارتكابها وصعوبة البحث والتحري عنها في عالم افتراضي، جعل العالم بمساحته الشاسعة رقعة جغرافية صغيرة لا تعترف بالحدود السياسية للدول.

وللإحاطة بذلك، سنتطرق في هذا المبحث إلى تعريف الإرهاب الإلكتروني (المطلب الأول)، ومميزاته وأهم جرائمه (المطلب الثاني).

### المطلب الأول: تعريف الإرهاب الإلكتروني

لقد أثار تعريف الإرهاب بشكل عام جدلا كبيرا في الفقه القانوني والتشريعات الجنائية الوطنية والاتفاقيات والمؤتمرات الدولية، ويعزى ذلك إلى عدة أسباب، لعل أهمها نعت البعض لأعمال العنف التي تقع من طرف حركات التحرر ضد العدو الأجنبي بالأعمال الإرهابية، ويكفي أن نستدل في هذا المقام بالموقف السلبي للولايات المتحدة الأمريكية التي ترى أن تعريف الإرهاب يجب أن يشمل جميع أعمال العنف الإرهابي الفردي، وصورا أخرى من العنف بما فيها أعمال العنف التي تمارسها المقاومة المسلحة من أجل تحرير أراضيها ونيل استقلالها[1].

ومن خلال ما سبق ذكره، سنتناول في هذا المطلب مشكلة تعريف الإرهاب (الفرع الأول)، ثم تعريف الإرهاب الإلكتروني (الفرع الثاني).

**الفرع الأول: مشكلة تعريف الإرهاب**

لقد انقسم فقهاء القانون حول مسألة تعريف الإرهاب إلى اتجاهين؛ اتجاه يرفض أنصاره تعريف هذه الظاهرة، مستندين في ذلك إلى عدة حجج، بينما يرى أنصار الاتجاه الثاني أن تعريف الإرهاب أمرٌ حتمي لتمييزه عن باقي ظواهر العنف المشابهة له سواء أكانت المشروعة أم غير المشروعة، وهذا ما سيتم تفصيله فيما سيتبع.

**أولاً- الاتجاه الفقهي الرافض لتعريف الإرهاب:**

يرى أنصار هذا المذهب أن الإرهاب غير قابل للتعريف، وحجتهم في ذلك أن أي محاولة لتعريفه لن تكون ملمة بجميع أشكاله وأساليبه، وأن أي تعريف لهذه الظاهرة إما أن يكون عاما يحتاج إلى تفسيرات أخرى أو يكون حصريا يشمل مجموعة من الجرائم الإرهابية، فيكون بذلك جامدا لا يستطيع مواكبة التطور المستمر لأشكال وأساليب الإرهاب[(2)].

كما أسس أنصار هذا المذهب رأيهم في رفض تعريف الإرهاب على اختلاف وجهات النظر الفكرية والسياسية والعقائدية للمهتمين بدراسة هذه الظاهرة، التي أصبح يفسرها كل واحد من الجهة أو الزاوية التي تخدم مصالحه[(3)]، وأن الدخول في موضوع تعريف الإرهاب يعتبر من المسائل غير المجدية في الفقه القانوني، مادام مفهومه مستقرّا في الأذهان[(4)].

وفي هذا الصدد يرى الفقيه "ولتر لكور" "Walter Laqueur" بأنه لا يوجد حاليا تعريف للإرهاب ولا يمكن تعريفه في المستقبل[(5)].

ويقول في هذا الشأن أيضا الفقيه "دنيال ستيفن" "Daniel Stephen" "إني لن أحاول تعريف الإرهاب لاعتقادي بأن مناقشة التعريف لن تحقق تقدما في دراسة المشكلة التي نتعامل معها"[(6)].

كما أقر مجلس الشيوخ الفرنسي في سنة 1984 أن أي محاولة لتعريف الإرهاب مآلها الفشل بسبب تعدد أشكاله وأساليبه، وأسبابه واتساع نطاقه، وغموض مفهومه[(7)].

وتجدر الإشارة إلى أن مندوبي الولايات المتحدة الأمريكية والكيان الصهيوني كانا من مؤيدي هذا المذهب في أشغال اللجنة الخاصة بدراسة مشكلة الإرهاب، التي أُنشِئت بموجب قرار الجمعية العام للأمم المتحدة رقم 3034 المؤرخ في 18 ديسمبر 1972، المتعلق بالتأكيد على قانونية النضال من أجل التحرر الوطني وإقامة لجنة خاصة لدراسة مشكلة الإرهاب الدولي[(8)]، حيث صرح ممثل الولايات المتحدة الأمريكية بأن "تعريف الإرهاب ليس ضروريا..."[(9)].

وقد تأثرت أيضا بهذا المذهب العديد من الدول المشاركة في المؤتمر الثامن المتعلق بمنع الجريمة ومعالجة المجرمين، المنعقد بهافانا سنة 1990، والمؤتمر التاسع المنعقد بالقاهرة سنة 1995، بتركيزها على ضرورة تعزيز التعاون الدولي لمكافحة الإرهاب، والبحث في أسبابه والعمل على إيجاد السبل الكفيل والفعالة لمعالجتها عوض تضييع الوقت في مشكلة تعريف الإرهاب[(10)].

### ثانياً- الاتجاه الفقهي المؤيد لتعريف الإرهاب:

على عكس الاتجاه الفقهي الرافض لتعريف الإرهاب، يري أنصار هذا الاتجاه كما أشرنا إليه سابقا بضرورة تعريف الإرهاب لوضع الحدود الفاصلة بينه وبين ظواهر العنف الأخرى التي يتقاطع معها في العديد من الخصائص، غير أنهم لم يتفقوا على تعريف واحد لهذه الظاهرة سواء أكان في الفقه الأجنبي أم الفقه العربي.

فقد عرف الفقيه "توم مالكيسون" "Tom Malkison" الإرهاب بأنه "الاستعمال المنسق للعنف أو التهديد به من أجل بلوغ أهداف سياسية"[11].

وما يؤخذ على هذا التعريف أنه يحصر مفهوم الإرهاب في استعمال العنف من أجل تحقيق أهداف سياسية فقط، بينما أهداف الإرهاب قد تكون سياسية أو اقتصادية أو اجتماعية أو عقائدية أو إعلامية من أجل لفت انتباه الرأي العام الداخلي والعالمي...إلخ.

وعرفه الفقيه "إريك دافيد" "Eric David" بأنه "عمل من أعمال العنف المسلح الذي يرتكب لتحقيق أهداف سياسية أو فلسفية أو إيديولوجية أو دينية. وهو كل اعتداء على الأرواح والأموال والممتلكات العامة أو الخاصة بالمخالفة لأحكام القانون الدولي العام، بما في ذلك الأحكام الأساسية لمحكمة العدل الدولية. أو هو الاستخدام غير المشروع للعنف أو التهديد بواسطة مجموعة أو دولة ضد فرد أو جماعة أو دولة ينتج عنه رعب يعرض للخطر أرواحا بشرية أو يهدد حريات أساسية ويكون الغرض منه الضغط على الجماعة أو الدولة لكي تغير سلوكها تجاه موضوع ما"[12].

وعرفه الدكتور "نبيل حلمي" بأنه "الاستخدام غير المشروع للعنف أو التهديد به بواسطة فرد أو مجموعة أو دولة ضد فرد أو مجموعة أو دولة، ينتج عنه رعب يعرض للخطر أرواحا بشرية أو يهدد حريات أساسية، يكون هدفه الضغط على الجماعة أو الدولة لتغيير سلوكها تجاه موضوع معين"[13].

ويرى الدكتور "عبد العزيز سرحان" أنّ الإرهاب هو "كل اعتداء على الأرواح أو الممتلكات أو الأموال العامة أو الخاصة، يقع بالمخالفة لأحكام القانون الدولي بمصادره المختلفة بما في ذلك نص المادة 38 من النظام الأساسي لمحكمة العدل الدولية، وبذلك يمكن النظر إليه على أساس أنه جريمة دولية، أساسها مخالفة القانون الدولي، وهو يقع كذلك تحت طائلة العقاب طبقا لقوانين سائر الدول"[14].

وقد انتقد هذا التعريف على أنه تعريف واسع يمكن أن يشمل العديد من الجرائم الدولية الأخرى التي لا تعتبر إرهابا، وهو أمر مخالف للموضوعية التي يتطلبها القانون ومساس بمبدأ العدالة[15].

فيما عرفه الأستاذ "محمود شريف بسيوني" بأنه "استراتيجية عنف محرم دوليا تحفزها بواعث عقائدية، وتتوخى أحداث عنف مرعبة داخل شريحة خاصة من مجتمع معين لتحقيق الوصول إلى السلطة، أو القيام بدعاية لمطلب أو لمظلمة بغض النظر عما إذا كان مقترفو العنف يعملون من أجل أنفسهم أو نيابة عنهم، أو نيابة عن دولة من الدول"[16].

وقد تم الأخذ بهذا التعريف من طرف لجنة الخبراء الإقليميين التي نظمت اجتماعاتها في الأمم المتحدة في فينا من 14 إلى غاية 18 مارس 1988[17]، إلا أنه انتقد أيضا كونه يركز على الدوافع السياسية للإرهاب فقط[18]، كما هو الشأن بالنسبة لتعريف الفقيه "توم مالكيسون".

**الفرع الثاني: تعريف الإرهاب الإلكتروني:**

في ظل غياب تعريف موحد للإرهاب العادي، تعددت أيضا تعريفات الإرهاب الإلكتروني. فقد عرفه قاموس "لاروس" "Larousse" بأنه "مجموعة من الهجمات الخطيرة (فيروسات، قرصنة،...إلخ) على حواسيب، شبكات وأنظمة الإعلام الآلي لمؤسسة أو هيئة، ترتكب لخلق فوضى عامة بهدف بث الرعب"[19].

وعرفه قاموس "كورديال" "Cordial" بأنه "مجموعة من الهجمات على شبكة الإنترنت، باستخدام الفيروسات والبرامج المخربة للبيانات."[20]

وبإمعان النظر في هذا التعريف، نجد أنه لم يحدد الهدف من الأفعال الإجرامية التي ترتكب عن طريق الإنترنت مقارنة بتعريف قاموس "لاروس"، وبذلك يخلط هذا التعريف بين الأفعال التي يرتكبها قراصنة المعلومات "Les Hackers"[21] بدافع الشهرة أو من أجل تحقيق مكاسب مادية، والأفعال التي يرتكبها الإرهابيون من أجل بث الرعب والخوف بين الناس.

وتجدر الإشارة إلى أن الإرهاب التقليدي، ظاهرة إجرامية قديمة قدم المجتمعات البشرية، غير أن الإرهاب الإلكتروني لم يظهر إلا حديثا بقلم الخبير "**باري كولين**" **"Barry Collin"** سنة 1996، والذي عرفه بأنه "التقاء العالم المادي مع العالم الافتراضي"[22].

ولكن ما يؤخذ على هذا التعريف أنه قد يشمل كل أنواع الإجرام المعلوماتي، في حين أن الإرهاب الإلكتروني له العديد من السمات التي تميزه عن باقي أنواع الجريمة الإلكترونية الأخرى.

وعرفه "دينينغ دوروثي" بأنه "الهجمات غير القانونية والتهديدات بالهجوم على أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها لتخويف أو إكراه حكومة أو شعبها، تعزيزا لأهداف سياسية أو اجتماعية" [23].

وعرفه الدكتور "مارك بوليت" "Mark Pollitt" بأنه "هجوم عمدي تحركه دوافع سياسية ضد نظم المعلومات وبرامج الكمبيوتر والبيانات عن طريق مجموعات فرعية وطنية أو عميل سري يؤدي إلى العنف ضد أهداف غير حربية"[24].

فيما عرفه الدكتور "أحمد فلاح العموش" بأنه "الإرهاب الناجم عن منتجات الحداثة الغربية وموجه لتدمير تلك المنجزات الحضارية والثقافية بأساليب إجرامية متطورة. ويستهدف المعلومات وأنظمة وبرامج الكمبيوتر والبيانات والتي ينتج عنها ارتكاب عنف ضد أهداف مدنية والتي تقوم بها مجموعات أو عملاء سريون"[25].

ونلاحظ أن الدكتور "مارك بوليت" والدكتور "أحمد فلاح العموش" يتفقان على أن الإرهاب الإلكتروني عمل إجرامي يرتكب من طرف مجموعات أو عملاء سرّيين، يستهدف النظم المعلوماتية وأنظمة

وبرامج الكمبيوتر والبيانات، ما يؤدي إلى عنف ضد أهداف مدنية غير عسكرية، بينما جرائم الإرهاب الإلكتروني قد ترتكب من طرف إرهابيين ذوي كفاءات عالية في مجال تقنية المعلومات من أجل إحداث عنف ضد أهداف مدنية أو عسكرية.

وعرفه البعض بأنه "العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من الدول أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه أو عرضه أو عقله أو ماله بغير حق، باستخدام الموارد المعلوماتية والوسائل الإلكترونية، بشتى صنوف العدوان وصور الإفساد"(26).

وعرف البعض بأنه "استخدام الموارد المعلوماتية المتمثلة في شبكات المعلومات وأجهزة الكمبيوتر والإنترنت، من أجل التخويف أو التهديد أو الإرغام لأغراض سياسية"(27).

وعرفه البعض بأنه "هجمات غير مشروعة أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونيا من أجل الانتقام أو ابتزاز أو إجبار الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية"(28).

في حين ذهب البعض إلى التمييز بين الإرهاب الإلكتروني، والأعمال الإرهابية التي تمارس على شبكة الإنترنت، فعرّفوا الإرهاب الإلكتروني بأنه "الأعمال والأنشطة التي يقوم بها أفراد أو جماعات باستخدام تكنولوجيا المعلومات والشبكة العنكبوتية قصد إحداث دمار للبنى التحتية المرتبطة والمدارة بواسطة مثل هذه التكنولوجيا كشبكات توزيع المياه والكهرباء، أنظمة الخدمات المصرفية، التسجيلات الصحية، الأنظمة العسكرية وغيرها من البنى التحتية التي من شأن تدميرها أن تحدث أضرار مباشرة وغير مباشرة بالمواطنين والدول"(29). وعرفوا الأعمال الإرهابية التي تمارس على شبكة الإنترنت بأنها "الأنشطة التي تقوم بها منظمات أو جماعات إرهابية تقليدية من أجل تدعيم أعمالها على أرض الواقع، وتشمل أنشطة التجنيد، الدعاية، المواد التعليمية الخاصة بالإعمال الإرهابية، التمويل، تبادل الأوامر...إلخ"(30).

كما عرفه "مركز حماية البنية التحتية القومية الأمريكية" بأنه "كل عمل إجرامي يتم التحضير له عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أو إيديولوجية"(31).

وعلى ضوء ما سبق ذكره، يمكننا تعريف الإرهاب الإلكتروني بأنه كل فعل إجرامي يرتكب ضد تقنية المعلومات أو بواسطتها لأغراض إرهابية أو التهديد بذلك، من أجل تحقيق أهداف محددة؛ قد تكون سياسية أو اقتصادية أو اجتماعية أو عقائدية أو إعلامية للفت انتباه الرأي العام لقضية معينة.

**المطلب الثاني: مميزات الإرهاب الإلكتروني وأهم جرائمه.**

إن التطور المستمر في وسائل تقنية المعلومات، وما حمله معه من مخاطر على الأمن المعلوماتي، جعل الإرهاب الإلكتروني يتميز بعدة خصائص عن باقي أشكال الإرهاب الأخرى التي ترتكب في العالم المادي، كما أدى بدوره إلى صعوبة حصر جميع جرائمه.

ولتوضيح ذلك، سنتطرق في هذا المطلب إلى أهم مميزات الإرهاب الإلكتروني (الفرع الأول)، وجرائمه الأكثر شيوعيا في العالم (الفرع الثاني).

**الفرع الأول: مميزات الإرهاب الإلكتروني:**

يمكننا إيجاز أهم مميزات الإرهاب الإلكتروني، فيما يلي:

**1- سهولة ارتكاب جرائمه:**

إذا كانت جرائم الإرهاب التقليدي تتطلب إمكانيات مادية وبشرية من المنظمات الإرهابية من أجل زعزعة الاستقرار الأمني والسياسي والاقتصادي، فإن جرائم الإرهاب الإلكتروني لا تتطلب لارتكابها سوى إرهابي يتحكم في تقنية المعلومات، وحاسوب أو هاتف محمول موصول بشبكة الإنترنت، وهو في مكان بعيد عن أعين الأجهزة الأمنية.

فبدلا من استعمال العنف بواسطة الأسلحة التقليدية والقنابل البشرية، التي تكلف هذه المنظمات أموالا كبيرة، أصبح اليوم بإمكانها الضغط على أزرار لوحة مفاتيح حاسب آلي موصول بشبكة الإنترنت من أي مكان في العالم لاختراق وتخريب النظم المعلوماتية للمنشآت الحيوية كمحطات الإمداد بالماء والطاقة الكهربائية، والمرافق النووية لإحداث خسائر بشرية ومادية، قد تفوق خسائر الحروب والكوارث الطبيعية[32].

**2- الإرهاب الإلكتروني من الجرائم العابرة للحدود:**

يعد الإرهاب الإلكتروني من أخطر الجرائم العابرة للحدود التي أصبحت تهدد أمن واستقرار جميع الدول، ولهذا شكل الرئيس الأمريكي السابق "بيل كلنتون" "Bill Clinton" لجنة خاصة لحماية البنية التحتية الحساسة في الولايات المتحدة الأمريكية، حيث قامت هذه اللجنة بتحديد العديد من المرافق الحيوية التي يمكن أن تتعرض إلى هجمات إلكترونية إرهابية كمصادر الطاقة والاتصالات...إلخ، كما جاء في التقرير الصادر عن وزارة الدفاع الأمريكية سنة 1997 أن شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في الولايات المتحدة الأمريكية، معرضة للهجوم من طرف أي جهة في العالم، تهدف إلى زعزعت الاستقرار الأمني للولايات المتحدة الأمريكية[33].

**3- صعوبة إثبات جرائم الإرهاب الإلكتروني:**

تعد جرائم الإرهاب الإلكتروني من الجرائم التي يصعب إثباتها، ويعود ذلك إلى عدة أسباب أهمها ما يلي:

أ- الطابع الدولي لجرائم الإرهاب الإلكتروني، فهي تتجاوز حدود الدولة لتشمل مجموعة من الدول مما يصعب تحديد مكان مرتكبي هذه الجرائم.

ب- الخبرة والكفاءة العالية التي يتمتع بها بعض الإرهابيين في مجال تقنية المعلومات، التي تمكنهم من محو أثار الجرائم التي يرتكبونها بكل سهولة في الفضاء الإلكتروني، ونقص الخبرة لدى بعض الجهات الأمنية والقضائية في اكتشاف هذه الجرائم[34].

ج- التطور التكنولوجي السريع في تقنية المعلومات، الذي صعب من الإلمام بجميع جوانبه واستخلاص الدليل الرقمي من بيئة افتراضية[35].

**الفرع الثاني: أهم جرائم الإرهاب الإلكتروني:**

تشير إحدى الدراسات إلى أن المنظمات الإرهابية استعملت تقنية المعلومات لبث الرعب والفزع ونشر أفكار التطرف والعنصرية حتى قبل ظهور شبكة الإنترنت، فقد قام "توم ميتزجر" "TomMetzger" اليمني المتطرف، مؤسس مجموعة المقاومة الإريانية البيضاء "White Aryan Resistance" بإنشاء شبكة بريدية إلكترونية سنة 1985 لنشر أفكاره المتطرفة والتواصل مع أتباعه[36].

ونظرا لتعدد جرائم الإرهاب الإلكتروني، سنركز في هذه الدراسة على أهم وأخطر هذه الجرائم التي لم تنص عليها المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات كما سنرى لاحقا في المطلب الأول من المبحث الثاني.

**1- اختراق النظم المعلوماتية:**

يعد هذا الاعتداء من أخطر الأساليب التي يمكن أن تلجأ إليها المنظمات الإرهابية للإضرار بالمصالح العامة والخاصة، فقد أصبح خطر اختراق الإرهابيين للنظم المعلوماتية للمرافق الحيوية كالمرافق النووية ومحطات الإمداد بالكهرباء والمياه والمستشفيات الهاجس الأكبر للدول، خاصة في ظل تمكن العديد من قراصنة المعلومات من اختراق النظم المعلوماتية لبعض المؤسسات التي تمتلك تكنولوجيا متطورة في مجال الأمن المعلوماتي في الدول المتطورة. فعلى سبيل المثال تمكن الهاركز الأمريكي "جوناثان جوساف جيمز" "Jonathan Joseph James" في سن الخامسة عشر من اختراق النظام المعلوماتي لمحطة أمريكية في الفضاء الدولي، الأمر الذي كبد شركة "ناسا" خسارة بقيمة 41 ألف دولار أمريكي، وسرقته لبرنامج إلكتروني بقيمة 1.7 مليون دولار بعد اختراقه للنظام المعلوماتي لوزارة الدفاع الأمريكية[37]. وتتم عملية اختراق النظم المعلوماتية في غالب الأحيان عن طريق الأفعال التالية:

**أ- التسلل:**

يشمل هذا الفعل كل الاختراقات للمواقع الرسمية للمؤسسات الحكومية أو المواقع الشخصية أو اختراق البريد الإلكتروني أو الاستيلاء على الأرقام السرية للمستخدمين، وتتم هذه العملية عن طريق تشغيل برنامج إلكتروني صغير يعرف باسم "**حصان طروادة**" في الحاسب الآلي للتجسس على كل ما يقوم به صاحبه، حيث يقوم هذا البرنامج بتسجيل كل بياناته السرية كرقم بطاقة الائتمان الخاصة به، والمكالمات التي يجريها مع غيره بواسطة هذا الحاسوب، بل وحتى كلمات السر التي يستعملها للدخول للإنترنت التي تمكن المجرم المعلوماتي من استخدامها. ومن أبرز الأمثلة على هذه العمليات في العالم، قيام مراهقين بالتسلل إلى الصفحة العنكبوتية للقواعد العسكرية للولايات المتحدة الأمريكية أثناء حرب الخليج مما أرعب الحكومة الأمريكية التي اعتقدت في بداية الأمر أنها تعرضت لعمل إرهابي[38].

ب- الإغراق بالرسائل الإلكترونية:

تتم هذه العملية عن طريق إرسال عدد كبير من الرسائل الإلكترونية ذات الحجم الكبير غير المفيدة دفعة واحدة وفي وقت متقارب قصد التأثير على السعة التخزينية للحواسيب الآلية المستهدف، ما يؤدي إلى توقفها عن العمل بسبب امتلاء منافذ الاتصال وكذا قوائم الانتظار، الأمر الذي ينتج عنه انقطاع الخدمة التي توفرها هذه الحواسيب[39].

ج- نشر الفيروسات الإلكترونية:

يقصد بالفيروسات الإلكترونية "برامج خارجية صنعت عمدا بغرض تغيير خصائص الملفات التي تصيبها، لتقوم بتنفيذ بعض الأوامر إما بالإزالة أو التعديل أو التخريب وما شابهها من عمليات الغرض منها إلحاق الضرر بحاسوب أو السيطرة عليه"[40].

وقد سميت هذه البرامج الإلكترونية بهذا الاسم، نظرا لتشابهها الكبير مع الفيروسات البيولوجية من حيث الانتقال والانتشار والقوة التدميرية، وقدرتها على تعديل مختلف البرامج، واستطاعتها التمييز بين البرامج السليمة والبرامج المصابة بالفيروس[41].

ويمكن تقسيم الفيروسات الإلكترونية التي يتم استخدامها للإضرار بالنظم المعلوماتية إلى خمسة (05) أنواع كالآتي:

- فيروسات الجزء التشغيلي للأسطوانة مثل فيروس "بران" "Brain"؛
- الفيروسات المصاحبة للبرامج التشغيلية؛
- الفيروسات المتطفلة مثل فيروس "كاسكاد" "Cascade"؛
- الفيروسات المتعددة الأنواع مثل فيروس "فليب" **"Flip"**؛
- أحصنة طروادة **"Les chevaux de Troie"**[42].

**2- استعمال الهواتف المحمولة في عمليات التفجير:**

يعد استعمال الهواتف المحمولة في عمليات التفجير عن بعد من أخطر أساليب الإرهاب الإلكتروني التي تلجأ إليها المنظمات الإرهابية لبث الرعب بين الناس، نظرا لقلة تكاليفها وسهولة استعمالها ووضعها في الأماكن العمومية التي تكثر فيها الحركة.

وتتم عمليات التفجير عن بعد بواسطة الهواتف المحمولة حسب خبراء تكنولوجيا الإعلام والاتصال من خلال الضغط على زر أمر الاتصال من هاتف لاسلكي إلى هاتف لاسلكي أخر، الذي يتحول بدوره إلى إشارات كهربائية. غير أنه بدلا من أن تصل هذه الإشارات إلى دائرة الصوت عن طريق السماعة، تحول مباشرة إلى دائرة التفجير[43].

## المبحث الثاني

## موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010 من الإرهاب الإلكتروني

لقد ألزمت الاتفاقية العربية جميع الدول الأطراف بأن تجرم في قوانينها الداخلية كل الأفعال التي نصت عليها في الفصل الثاني منها، بما في ذلك الأفعال المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات، وتبنيها أيضا لحزمة من التدابير الإجرائية، وكذا تعزيزها لجهود التعاون القانوني والقضائي بينها لمكافحة كافة هذه الأفعال الخطيرة بصورة فعالة.

ولتوضيح موقف الاتفاقية العربية لمكافحة جرائم تقنية المعلومات من الإرهاب الإلكتروني، سنتطرق في هذا المبحث إلى صوره التي نصت عليها هذه الاتفاقية (المطلب الأول)، والآليات التي اعتمدتها لمكافحة هذه الجريمة (المطلب الثاني).

### المطلب الأول: صور الإرهاب الإلكتروني التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات.

بإلقاء نظرة فاحصة على المادة 15[44] من هذه الاتفاقية نجد أنها قد حصرت الإرهاب الإلكتروني في ثلاث صور؛ تتمثل الأولى في نشر أفكار التطرف وطرق صناعة المتفجرات والفتن والنعرات والاعتداء على الديانات، والثانية في تمويل الأعمال الإرهابية والتدريب عليها، أما الثالثة فتتمثل في تسهيل الاتصال بين المنظمات الإرهابية.

**1- نشر أفكار التطرف وطرق صناعة المتفجرات والفتن والاعتداء على الديانات والمعتقدات:**

يتميز النشر في العالم الافتراضي بالسرعة والحرية المطلقة غير المقيدة بإجراءات معينة، ما عدا تلك المتعلقة بحجز نطاق الاسم والمساحة الضرورية لدى أحد مقدمي الخدمات، على عكس النشر في العالم المادي الذي يتطلب إجراءات محددة كإيداع المصنف والالتزام باحترام النظام العام والآداب العامة...إلخ[45].

ونظرا لسهولة النشر الإلكتروني على شبكة الإنترنت، ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف في المادة 15 منها بتجريم نشر فكر التطرف والغلو الذي يعتبر أحد أهم العوامل المغذية للعنف والإرهاب سواء أكان عن طرق الفتاوى المسموعة أم السمعية البصرية أو المقروءة، وطرق صناعة المتفجرات وكيفية استعمالها في الأعمال الإرهابية، وكذا نشر الفتن الطائفية والسياسية والاعتداء على الديانات بالسب والتحقير و السخرية أو غير ذلك من الأفعال التي تمس بحرية المعتقد.

وتعد المواقع الإلكترونية المتطرفة التي يقصد بها "تلك المواقع التي تتيح المعلومات على شبكة الإنترنت وتساعد على نشر وتداول الأفكار الضالة، والتحريض على استخدام العنف من أجل تحقيق أهداف خاصة بالقائمين عليها تحت مظلات ومسميات دينية وسياسية، بهدف إلحاق أكبر ضرر بالآخرين

دولا وشعوبا"[46]، إحدى أهم الأساليب التي تستعملها المنظمات الإرهابية لنشر أفكار التطرف وطرق صناعة المتفجرات والفتن والاعتداء على الديانات والمعتقدات...إلخ.

وفي ظل التزايد المستمر لعدد مستخدمي الإنترنت في العالم، الذين فاق عددهم 3.42 مليار مستخدما في العالم خلال سنة 2016[47]، لجأت المنظمات الإرهابية إلى إنشاء العديد من هذه المواقع الإلكترونية المتطرفة، فقد أحصى الخبيران في الدراسات الإعلامية "فيليب سيب" و"دانا جانبك" في كتابهما "الإرهاب الدولي والإعلام الجديد"، 2000 موقعا إلكترونيا إرهابيا سنة 1997، و4350 موقعا في مطلع سنة 2005، و6000 موقعا في سنة 2008، ليتجاوز حاليا 60 ألف موقعا إلكترونيا إرهابيا[48].

وإلى جانب المواقع الإلكترونية المتطرفة، تستغل المنظمات الإرهابية شبكات التواصل الاجتماعي[49]، لارتكاب الأفعال المنصوص عليها في المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، فقد بينت إحدى الدراسات أن نسبة 80 % من الإرهابيين تم تجنيدهم عن طريق هذه الشبكات[50] خاصة في ظل تزايد إقبال فئة الشباب عليها في الدول العربية.

وفي هذا الإطار تشير أيضا إحدى الدارسات إلى أن شبكة التواصل الاجتماعي "فيسبوك" "Facebook" هي الشبكة الأكثر رواجا في الدول العربية مقارنة باقي شبكات التواصل الاجتماعي الأخرى، ففي بداية سنة 2017 وصل عدد مستخدميها إلى حوالي 156 مليون مستخدم فعال ومتفاعل، ويليها في المرتبة الثانية شبكة التواصل الاجتماعي "إنستقرام" "Instagram" بمجموع 16.6 مليون مستخدما، ثم شبكة التواصل الاجتماعي "لينكد إن" "Linkedin" بمجموع 11.1 مليون مستخدما[51].

ورغم إيجابيات هذه الشبكات في تبادل المعارف والثقافات وتسهيلها للاتصال بين الأصدقاء والأقارب، إلا أنها أصبحت تشكل فضاءً افتراضيا للإرهابيين للتواصل فيما بينهم للبحث عن السند والمشورة، خاصة أنها تتيح لمستخدميها إمكانية الولوج إليها بأسماء مستعارة[52].

وجدير بالذكر أن بعض الدول كالصين، إيران، كوريا الشمالية، بنجلاديش، أفغانستان، باكستان، تايلاند، وكوريا الجنوبية، رغم الإجراءات التي اتخذتها لحجب بعض شبكات التواصل الاجتماعي كفيسبوك وتويتر[53]، إلا أن مستخدمي هذه الشبكات تمكنوا من الولوج إليها بواسطة تقنيات تجاوز حجب المواقع الإلكترونية مثل تقنية "VPN"، حيث كشفت إحصائيات "eMarketer" في سنة 2012، أن 35.5 مليون صيني ينشط على شبكة التواصل الاجتماعي "تويتر" رغم حجب الصين لهذه الشبكة، واستبدالها للمواقع الإلكترونية التي قامت بغلقها أو حجبها بمواقع محلية أخرى كمحرك البحث "بايدو" وموقع "يوكو" لمقاطع الفيديو[54].

ولا يقف الأمر عند صور النشر التي عددتها المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، بل أن المنظمات الإرهابية أصبحت تستخدم هذه التقنية أيضا لنشر فيديوهات وصور عن أبشع الجرائم التي يرتكبها الإرهابيون لبث الرعب والخوف بين الناس والظهور بمظهر القوة.

2- تمويل الأعمال الإرهابية والتدريب على ارتكابها بواسطة تقنية المعلومات:

يعرف تمويل الإرهاب بأنه "أي دعم مالي في مختلف صوره يقدم إلى الأفراد أو المنظمات التي تدعم الإرهاب أو تقوم بالتخطيط لعمليات إرهابية. وقد يأتي هذا التمويل من مصادر مشروعة كالجمعيات الخيرية مثلا أو مصادر غير مشروعة مثل تجارة البضائع التالفة أو تجارة المخدرات"[55].

وعرّفته الاتفاقية العربية لمكافحة غسيل الأموال وتمويل الإرهاب لعام 2010 بأنه "جمع أو تقديم أو نقل الأموال بأي وسيلة مباشرة أو غير مباشرة لاستخدامها كليا أو جزئيا لتمويل الإرهاب وفقا لتعريفات الإرهاب الواردة في الاتفاقية العربية مع العلم بذلك"[56].

وتعد تقنية المعلومات من أهم الوسائل التي سهلت تمويل الإرهاب بعيدا عن أعين السلطات الأمنية سواء أكان عن طريق المواقع الإلكترونية الإرهابية أم شبكات التواصل الاجتماعي التي يتم فيها اصطياد الأشخاص لجمع التبرعات المالية أم عن طريق قرصنة الحسابات البنكية وبطاقات الائتمان لتحويل الأموال من حساب إلى حساب آخر.

وللإشارة تتعدد الطرق الإلكترونية التي يمكن بواسطتها سرقة الأموال، ولعل أهمها البريد الإلكتروني المزعج أو غير المرغوب فيه، أو ما يعرف باسم "سبام" "SPAM" الذي يقصد به إرسال كم هائل من الرسائل غير المرغوب فيها إلى العديد من الأشخاص، التي تكون في غالب الأحيان الرسالة نفسها لإيهامهم بأنها رسالة مهمة تحمل اسم البنك، وتتضمن تحذيرا لضحاياها أن حساباتهم سوف يتم غلقها إذا لم يتم تفعيلها، ثم يتم توجيه الضحايا إلى صفحة أخرى مزورة تتشابه مع صفحات البنوك الخاصة بهم، وفي هذه الصفحة المزورة يطلب منهم كل البيانات المتعلقة ببطاقة الائتمان، وكل ما يسجلونه سيصل إلى البريد الإلكتروني للمجرم[57].

أما عن استعمال المنظمات الإرهابية لهذه التقنية لتدريب الإرهابيين، فيمكننا القول بأن الإنترنت أصبح مركزا افتراضيا لتدريب الإرهابيين عن بعد عن كيفيات استعمال الأسلحة ومختلف أساليب القتل والعنف والتخريب والتفجير لبث الرعب والخوف بين الناس كقطع الرؤوس واختطاف الطائرات واستعمال الأحزمة الناسفة وتلغيم السيارات وزراعة المتفجرات في الأماكن العمومية، بل وحتى طرق اختراق النظم المعلوماتية للمرافق الحكومية والمؤسسات المصرفية.

3- تسهيل الاتصال بين المنظمات الإرهابية:

إلى جانب إلزام الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتجريم نشر أفكار التطرف وطرق صناعة المتفجرات والفتن والنعرات والاعتداء على الديانات، وتمويل الأعمال الإرهابية والتدريب عليها، ألزمتها أيضا بتجريم كل الأفعال التي من شأنها تسهيل الاتصال بين المنظمات الإرهابية عن طريق مختلف وسائل الاتصال لمنعها من تبادل الأفكار والتنسيق والتعاون بينها لتنفيذ مخططاتها الإجرامية.

ويبدو من الوهلة الأولى أن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أغفلت تجريم العديد من الأفعال الأشد خطورة من الأفعال التي نصت عليها في المادة 15 منها التي ترتكب بواسطة

تقنية المعلومات لأغراض إرهابية كاختراق النظم المعلوماتية للأجهزة الحكومية ومختلف المؤسسات الحيوية كالمرافق النووية، والمطارات، ومحطات المياه والطاقة الكهربائية، والتجسس الإلكتروني، وإنشاء المواقع الإلكترونية المتطرفة، واستعمال أجهزة الاتصال المحمولة لتفجير القنابل عن بعد...إلخ، غير أنه وبالرجوع إلى المادة 22 من هذه الاتفاقية، نجدها تلزم الدول الأطراف بتطبيق الصلاحيات والإجراءات المحددة في الفصل الثالث منها، المتعلق بالأحكام الإجرائية على الجرائم التي نصت عليها في المواد من 06 إلى 19، أو أي جريمة أخرى ترتكب بواسطة تقنية المعلومات، الأمر الذي يسوقنا للقول بأن هذه الاتفاقية وسعت من مجال تطبيق أحكامها لتشمل جميع الجرائم التي ترتكب بواسطة هذه التقنية بما في ذلك مختلف جرائم الإرهاب الإلكتروني التي لم تنص عليها المادة 15 منها.

وربما يرجع تركيز الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على صور الإرهاب الإلكتروني المحددة في المادة 15 منها، إلى كثرة انتشار هذه الجرائم في البيئة الرقمية، خاصة على شبكة الإنترنت التي باتت تعتمد عليها المنظمات الإرهابية إلى حد بعيد كسلاح افتراضي عابر للحدود ومتعدد الاستخدامات من خلال مواقعها الإلكترونية أو مواقع إلكترونية أخرى كموقع **"يوتيوب"** "youtube" الشهير أو شبكات التواصل الاجتماعي.

## المطلب الثاني: آليات مكافحة الإرهاب الإلكتروني التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

إن مكافحة الإرهاب الإلكتروني باعتباره من أخطر الجرائم العابرة للحدود التي أصبحت تهدد الأمن المعلوماتي، تقتضي تبنّي الدول في قوانينها الداخلية لمجموعة من الأحكام الإجرائية، وتكثيفها لجهود التعاون القانوني والقضائي والتقني فيما بين الدول.

ومن هذا المنطلق، نصت هذه الاتفاقية على حزمة من الآليات الفعالة لمكافحة هذه الجريمة، التي سنتطرق إليها في هذا المطلب بالتفصيل من خلال (الفرع الأول) المتعلق بالآليات الإجرائية، و(الفرع الثاني) الذي يتناول آليات التعاون القانوني والقضائي بين الدول الأطراف.

### الفرع الأول: الآليات الإجرائية التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

يمكننا إيجاز الآليات الإجرائية التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات فيما يلي:

**1- الحفظ العاجل للبيانات المعلوماتية المخزنة والأمر بتسليمها:**

تعرف البيانات المعلوماتية حسب هذه الاتفاقية بأنها "كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها"[58].

وعرفها المشرع السعودي بأنها "المعلومات أو الأوامر، أو الرسائل، أو الأصوات، أو الصور التي تعد أو التي سبق إعدادها، لاستخدامها في الحاسب الآلي، وكل ما يمكن تخزينه، ومعالجته، ونقله وإنشاؤه بوساطة الحاسب الآلي، كالأرقام والحروف والرموز وغيرها"[59].

أما التحفظ العاجل للبيانات المعلوماتية، فيقصد به "توجيه السلطة المختصة لمزود الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته في انتظار اتخاذ إجراءات قانونية أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية"[60].

وعليه يقتضي الحفظ أن تكون البيانات المعلوماتية المخزنة في تقنية معلومات، محمية بشكل آمن من كل المخاطر التي قد تؤدي إلى المساس بسلامتها كالتغيير أو التعديل أو الحذف...إلخ، ولا يعني الحفظ بالضرورة أن تكون البيانات المخزنة مجمدة، لا يمكن لأي كان النفاذ إليها أو استخدامها أو استخدامُ نسخٍ منها، بل يمكن للشخص الذي يوجه له الأمر القيام بذلك في حدود ما يسمح به أمر الحفظ[61].

ويعد هذا الإجراء من أهم الإجراءات التي نصت عليها الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في المادة 23 منها، التي ألزمت بموجبها الدولة الأطراف باتخاذ التدابير التشريعية اللازمة لما تقتضيه إجراءات التحقيق في الجريمة الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني لتمكين السلطات المختصة من توجيه الأمر لشخص بحفظ البيانات المعلوماتية المخزنة التي في حوزته أو تحت سيطرته لمدة أقصاها 90 يوما تكون قابلة للتجديد خاصة إذا كانت هذه الأخيرة معرضة للفقدان أو التعديل، واتخاذ الإجراءات الضرورية التي من شأنها الحفاظ على سرية المعلومات المخزنة طيلة الفترة القانونية المنصوص عليها في قوانينها الداخلية[62].

كما تلزم هذه الاتفاقية الدول المتعاقدة باعتماد إجراءات تستطيع من خلالها السلطات المختصة من توجيه الأمر إلى أي شخص كان على إقليمها قصد تقديم البيانات التي بحوزته سواء أكانت المخزنة في تقنية معلومات أم في دعامة تخزين كالأقراص المرنة والصلبة والمدمجة والرقاقات الإلكترونية...إلخ، أو إلى أي مزود خدمة لتسليم معلومات المشتركين في الخدمة المقدمة التي بحوزته أو تحت سيطرته[63].

ولكن ما يؤخذ على هذه الاتفاقية أنها لم تحدد عدد مرات تمديد مدة حفظ البيانات المعلوماتية المخزنة التي نصت عليها في المادة 23 منها، وإنما اكتفت بعبارة "90 يوما قابلة للتجديد"، كما لم تعرف "مزودي الخدمة" على عكس اتفاقية بودابست لسنة 2001 المتعلقة بالجرائم المعلوماتية التي عرفت هذه الكيانات على النحو التالي:

- "أي كيان عام أو خاص يقدم لمستغلي خدماته القدرة على الاتصال بواسطة منظومة معلوماتية؛

- أي كيان آخر يقوم بمعالجة أو تخزين معطيات معلوماتية لفائدة خدمة الاتصال المذكورة أو لمستعمليها"[64].

وهو التعريف الذي أخذ به المشرع الجزائري في المادة الثانية من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال.

فيما حصر المشرع الفرنسي مزودي الخدمة في ثلاثة كيانات؛ تتمثل في مقدمي خدمة التوصيل بشبكات الاتصال الإلكترونية "Les aux réseaux de communications électroniques

"fournisseurs d'accès"، مقدمي خدمة الإيواء "Les Fournisseurs d'hébergement"، مقدمي المضمون أو النشر "Les Fournisseurs de contenus ou les éditeurs"[65].

**2- تفتيش المعلومات المخزنة:**

يعتبر تفتيش البيانات المخزنة في تقنية معلومات أحد أهم الإجراءات للكشف عن ملابسات الجريمة والوصول إلى مرتكبيها، ولهذا تلزم الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف باتخاذ التدابير التشريعية اللازمة حتى تتمكن سلطاتها المختصة من تفتيش تقنية معلومات أو جزء منها أو إحدى وسائط تخزين المعلومات الإلكترونية[66].

ولما كان تفتيش المعلومات المخزنة في تقنية المعلومات يمس بالحياة الخاصة للأشخاص، أحاطته معظم التشريعات الجنائية بضوابط موضوعية وشكلية. وفي هذا الإطار أجاز المشرع الجزائري بموجب المادة 05 من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، للسلطات القضائية وضباط الشرطة القضائية تفتيشهم لمنظومة معلوماتية أو جزء منها أو المعلومات المخزنة فيها للوقاية من جرائم الإرهاب والتخريب أو المساس بأمن الدول، شريطة التقيد بضوابط التفتيش المنصوص عليها في قانون الإجراءات الجزائية، كما خول لهذه السلطات في المادة نفسها من ذات القانون تسخير أي شخص له دراية بعمل المنظومة المعلوماتية محل التفتيش[67]. واستثناءً عن القاعدة التي لا تجيز البدء في إجراء التفتيش قبل الخامسة (05) صباحا وبعد الثامنة (08) مساء في قانون الإجراءات الجزائية، أجاز المشرع الجزائري في جرائم الإرهاب للسلطات المختصة بإجراء التفتيش والمعاينة والحجز في أي ساعة من الليل أو النهار، وفي أي محل سواء أكان سكنيا أم غير سكني بعد الحصول على إذن مسبق من وكيل الجمهورية المختص إقليميا[68].

**3- ضبط المعلومات المخزنة (الحجز):**

يعرف الضبط بأنه "العثور على أدلة خاصة بالجريمة التي يباشر التحقيق بشأنها والحفظ على هذه الأدلة، والضبط هو الغاية من التفتيش ونتيجته المباشرة المستهدفة، ولذلك يتعين عند إجرائه أن تتوفر فيه القواعد نفسها التي تنطبق بشأن التفتيش، ويؤدي بطلان التفتيش إلى بطلان الضبط"[69].

غير أن محل الضبط في مجال الجرائم الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني، أثار جدلا كبيرا، وانقسم بشأنه فقهاء القانون إلى اتجاهين؛ الاتجاه الأول يرى أنصاره أن المعلومات المعالجة إلكترونيا في عالم افتراضي غير مادي لا يمكن أن تكون محلا للضبط إلا بعد نقلها على كيان مادي ملموس، عن طريق التصوير، أو بنقلها بواسطة مختلف دعائم التخزين الإلكترونية. فيما ذهب أنصار الاتجاه الثاني إلى أن المعلومات المعالجة إلكترونيا ما هي إلا ذبذبات إلكترونية، أو موجات كهرومغناطيسية، قابلة للتسجيل والحفظ والتخزين، يمكن نقلها وبثها واستقبالها وإعادة إنتاجها، وبذلك لا يمكن إنكار وجودها المادي[70].

ونظرا لأهمية هذا الإجراء في مكافحة الجريمة الإلكترونية، نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في 27 منها على ضرورة اعتماد الدول الأطراف لإجراءات تمكن السلطات المختصة

من ضبط وتأمين تقنية المعلومات أو جزء منها أو وسائط تخزين المعلومات كالأقراص المرنة والصلبة والمدمجة والرقاقات الإلكترونية...إلخ، ونسخ المعلومات والاحتفاظ بها ومحوها أو إزالتها من التقنية التي اكتشفت فيها أو منع أي شخص آخر من الوصول إليها، وتمكين هذه السلطات من الاستعانة بالأشخاص الذين لهم خبرة ومعرفة في هذا المجال[71].

وتجدر الإشارة إلى أن المشرع الجزائري كان سباقا في النص على هذه الإجراءات في القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في المواد من 06 إلى 08.

**4- الجمع الفوري لمعلومات تتبع المستخدمين:**

إلى جانب الإجراءات السابق ذكرها، ألزمت هذه الاتفاقية الدول الأطراف باتخاذ التدابير اللازمة التي من شأنها أن تمكن السلطات المختصة من جمع أو تسجيل المعلومات المتعلقة بتتبع المستخدمين عن طريق مختلف الوسائل الفنية وتلزم مزودي الخدمة في حدود اختصاصهم أيضا للقيام بذلك مع الحفاظ على سرية هذه المعلومات[72]، ولكنها لم تحدد الشروط القانونية الواجب اتخاذه لجمع وتسجيل المعلومات ما عدا إلزامها الدول الأطراف بتبنّي إجراءات لإلزام مزودي الخدمة بالحفاظ على سرية المعلومات[73].

**5- اعتراض بيانات المحتوى:**

تنص المادة 29 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، على إلزامية تبني الدول الأطراف في تشريعات الداخلية للتدابير اللازمة، لتمكين السلطات المختصة من اعتراض بيانات المحتوى في ما يتعلق ببعض الجرائم المنصوص عليها في قوانينها الداخلية.

وهنا تجب الإشارة إلى أن هناك نوعين من البيانات التي يمكن جمعها أو تسجيلها، وهي "بيانات المحتوى" و"بيانات الحركة"، إلا أن هذه الاتفاقية لم تعرف أيّ منهما، في حين عرفت اتفاقية بودابست لسنة 2001 "بيانات الحركة" بأنها "أي بيانات كومبيوتر متعلقة باتصال عن طريق نظام الكومبيوتر والتي تنشأ عن نظام كومبيوتر يشكل جزءا في سلسلة الاتصالات توضح المنشأ والوجهة، الزمن، والتاريخ، والحجم، والمدة أو نوع الخدمة الأساسية"[74]، ولكنها لم تعرف هي الأخرى "بيانات المحتوى"، غير أنها تشير إلى محتوى الاتصال أي الرسالة أو المعلومات التي ينقلها الاتصال، ونظرا لخطورة هذا الإجراء ومساسه بحق الحياة الخاصة، فإنه يقتصر على بعض الجرائم الخطيرة المحددة في القوانين الداخلية للدول[75].

وفي هذا الصدد نص المشرع الجزائري في المادة 03 من القانون رقم 04/09 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على أنه "مع مراعاة الأحكام القانونية التي تضمن سرية المراسلات والاتصالات يمكن لمقتضيات حماية النظام العام أو مستلزمات التحريات أو التحقيقات القضائية الجارية وفقا للقواعد المنصوص عليها في هذا القانون وضع ترتيبات تقنية لمراقبة الاتصالات الإلكترونية وتجميع وتسجيل محتواها في حينها والقيام بإجراءات التفتيش والحجز داخل منظومة معلوماتية"[76].

كما أجاز للسلطات المختصة باللجوء إلى المراقبة الإلكترونية المنصوص عليها في هذه المادة 03 للوقاية من الجرائم الإرهابية والتخريبية، أو في حالة توفر معلومات تفيد باحتمال وقوع اعتداءات إلكترونية على منظومة معلوماتية تهدد النظام العام أو الدفاع الوطني أو مؤسسات الدولة أو الاقتصاد الوطني، أو في الحالات التي يصعب فيها الوصول إلى الحقيقة دون اللجوء إلى هذا الإجراء[77].

وقد قيد المشرع الجزائري إجراء المراقبة الإلكترونية في الجرائم الإرهابية أو التخريبية بشرط حصول ضباط الشرطة القضائية المنتمين إلى الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال على إذن من النائب العام لدى مجلس قضاء الجزائر العاصمة لمدة 06 أشهر قابلة للتجديد بناء على تقرير يبين الترتيبات التقنية لإجراء هذه المراقبة[78]، ولكنه لم يحدد مدة تمديد الإذن بالمراقبة.

**الفرع الثاني: آليات التعاون القانوني والقضائي لمكافحة جرائم الإرهاب الإلكتروني**

يقصد بالتعاون القضائي الدولي "مجمل الإجراءات التي تتخذها السلطات القضائية داخل الدولة بصدد جريمة محددة أو مجرمين محددين (متهمين أو محكوم عليهم) والمنصوص عليها في الاتفاقيات الدولية التي تكون الدول طرفا فيها بمقتضى التشريعات الوطنية النافذة "[79].

**1- تسليم المجرمين:**

يعرف تسليم المجرمين بأنه "ذلك الإجراء القانوني الذي تقوم به دولة ما لتسليم شخص متواجد على إقليمها إلى دولة أخرى تطلب تسليمه لمحاكمته أو لتنفيذ العقوبة المحكومة بها أو كإجراء وقائي"[80].

وعرفه نظام روما الأساسي بأنه "نقل دولة ما شخصا إلى دولة أخرى بموجب معاهدة أو اتفاقية أو تشريع وطني"[81].

وتتجلى أهمية هذا الإجراء في عدم توفير المكان الذي يفلت فيه مقترفو هذه الجرائم من العقاب وتفادي خطرهم على أمن واستقرار الدول، ولهذا ألزمت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الدول الأطراف بتسليم مرتكبي الجرائم التي نصت عليها في الفصل الثالث، بما فيها الجرائم المتعلقة بالإرهاب والمرتبكة بواسطة تقنية المعلومات المحددة في المادة 15 منها، شريطة أن تكون عقوبة هذه الجرائم في التشريعات الجنائية للدول الأطراف سالبة للحرية تساوي أو تزيد عن سنة أو بعقوبة أشد منها. وفي حال اشتراط إحدى الدول الأطراف وجود معاهدة لتسليم المجرمين، وتقدمت إليها دولة أخرى طرف لا تربطها بها اتفاقية ثنائية في هذا الشأن، أو عدم اشتراط الدول الأطراف لوجود معاهدة لتسليم المجرمين، فإن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات تعتبر كأساس قانوني لتسليم المجرمين، كما أجازت هذه الاتفاقية لكل دولة طرف أن تمتنع عن تسليم مواطنيها على أن تتعهد للدول الأطراف الأخرى التي تتقدم إليها بطلب الملاحقة بأن توجه الاتهام لمواطنيها الذين ارتكبوا جرائم إلكترونية في هذه الدول، ومباشرتها لإجراءات التحقيق والمحاكمة والتزامها بإعلام الدولة الطالبة بما تم اتخاذه بشأن طلبها المتعلق بالملاحقة[82].

2- المساعدة المتبادلة بين الدول الأطراف:

نصت الاتفاقية العربية لمكافحة جرائم تقنية المعلومات على جملة من الإجراءات لتنظيم طلبات المساعدة المتبادلة بين الدول الأطراف، يمكننا أن نوجزها في ما يلي:

- يتعين على كل دولة طرف أن تقوم بتعين سلطة مركزية تعنى بإرسال ودراسة طلبات المساعدة المتبادلة والإجابة عليها وتنفيذها أو تقديمها إلى السلطات المختصة لتنفيذها، على أن يتم قيد هذه السلطة في سجل خاص تعده الأمانة العامة لوزراء الداخلية العرب والأمانة الفنية لوزراء العدل العرب لهذا الغرض[(83)]، غير أنه في الحالات المستعجلة يمكن أن توجه أي دولة طرف طلب المساعدة مباشرة إلى السلطة القضائية للدولة المطلوب منها المساعدة، مع التزام الدولة الطالبة بإرسال نسخة من هذا الطلب إلى السلطة المركزية للدولة المطلوب منها المساعدة. وفي وحالة عدم اختصاص السلطة القضائية تحيل هذه الأخيرة طلب المساعدة إلى السلطة المختصة شريطة إعلامها للدولة الطالبة بذلك فورا، كما أجازت هذه الاتفاقية للدول الأطراف إرسال طلبات المساعدة إلى بعضها البعض عن طريق المنظمة الدولية للشرطة الجنائية "INTERPBOL"[(84)].

- توجه طلبات المساعدة المتبادلة من الدولة الطرف الطالبة للمساعدة إلى الدولة المطلوب منها بشكل خطي كقاعدة عامة، غير أنه يجوز أن ترسل هذه الطلبات في الحالات المستعجلة عن طريق وسائل الاتصال الحديثة كالفاكس أو البريد الإلكتروني مع مراعاة أمن وسرية الاتصالات بين الأجهزة المختصة للدول التي تقدمت بطلب المساعدة والدولة التي تلقت هذا الطلب كاستعمال طريقة تشفير المعلومات مثلا[(85)].

ويقصد بالتشفير "عملية تحويل المعلومات إلى شيفرات غير مفهومة (تبدو غير ذات معنى) لمنع الأشخاص غير المرخص لهم من الاطلاع على المعلومات أو فهمها، ولهذا تنطوي عملية التشفير على تحويل النصوص العادية إلى نصوص مشفرة"[(86)].

إن هذه التقنية تعتبر من أهم التقنيات المستعملة لحماية المعلومات السرية المخزنة في الحاسب الآلي أو نقلها عبر الشبكات غير المأمونة كشبكة الإنترنت، حتى لا يتمكن الأشخاص غير المرخص لهم من الاطلاع عليها[(87)]، حيث تتم هذه العملية إما عن طريق التشفير التقليدي أو المتماثل الذي يعتمد على مفتاح واحد لعملية التشفير وفك التشفير للبيانات أو عن طريق تشفير المفتاح العام الذي يُسْتخْدَم فيه مفتاحان؛ مفتاح عام لتشفير الرسائل ومفتاح خاص لفتح الرسائل المشفرة[(88)].

- خضوع طلب المساعدة للشروط المحددة في قانون الدولة الطرف المطلوب منها المساعدة أو في الاتفاقيات الثنائية المتعلقة بالمساعدة المتبادلة بما في ذلك الأسس التي يمكن للدول المتلقية لطلب المساعدة الاعتماد عليها لرفض هذا الطلب[(89)]، كما يجوز للدولة المطلوب منها المساعدة رفض هذا الطلب إذا كان قانونها الداخلي يعتبر هذه الجرائم من قبيل الجرائم السياسية أو أن تنفيذ طلب المساعدة سيشكل انتهاكا لسيادتها أو خطرا على أمنها أو مصالحها الجوهرية[(90)].

- يجوز للدولة الطرف المطلوب منها المساعدة تأجيل الإجراءات التي اتخذتها بشأن طلب المساعدة إذا كان من شأنها التأثير سلبا على التحقيقات التي تقوم بها أجهزتها المختصة. وقبل رفض أو تأجيل المساعدة تقرر هذه الأخيرة بعد استشارة الدولة الطالبة ما إذا كانت ستقدم لها المساعدة بشكل جزئي أو بشروط خاصة، كما تلتزم بإعلامها بنتائج تنفيذ هذا الطلب. وفي حالة رفضه أو تأجيله يتعين عليها أيضا إعلامها بأسباب الرفض أو التأجيل[91].

- إذا تقدمت دولة طرف بطلب مساعدة إلى دولة أخرى طرف، تجيز هذه الاتفاقية للدول المطلوب منها المساعدة أن تشترط الحفاظ على سرية هذه المعلومات المقدمة، وأن تستخدمها في حدود الطلب ولا تستخدمها في تحقيقات أخرى لا تتعلق بالجريمة موضوع التحقيق. وإذا لم تستطِعْ الدولة الطالبة الالتزام بالحفاظ على سرية المعلومات، يجب عليها ـ كما سبقت الإشارة ـ إعلامُ الدولة المطلوب منها تقديم المساعدة[92].

**2-1-مجالات المساعدة المتبادلة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات:**

تتمثل مجالات المساعدة المتبادلة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في ما يلي:

**أ- التقديم التلقائي للمعلومات بين الدول الأطراف:**

أجازت هذه الاتفاقية على غرار اتفاقية بودابست لسنة 2001 للدول الأطراف أن تقدم لبعضها البعض بصفة تلقائية لمعلومات تحصلت عليها من خلال التحقيقات التي تقوم بها مصالحها المختصة بدون طلب مسبق للمساعدة في إطار التعاون من أجل مواجهة الجريمة الإلكترونية والإرهاب الإلكتروني[93]، كما أجازت هذه الاتفاقية للدولة التي تحيل المعلومات بصفة عرضية أن تطلب من الدول التي أحالت لها المعلومات أن تحافظ على سريتها في حالة ما إذا كانت هذه المعلومات حساسة أو إذا ما تم الكشف عنها قد تتعرض المصالح الجوهرية للدولة المقدمة للمعلومات للخطر. وإذا كشف التحقيق المسبق أن الدولة الطرف المتلقية للمعلومات لا تستطيع الالتزام بالسرية كما لو كانت هذه المعلومات مطلوبة كدليل في محاكمة علنية[94]، فيتعين عليها إعلام الدولة التي أحالت إليها هذه المعلومات، أما إذا قبلت المعلومات بشرط الحفاظ على سريتها فيجب عليها التقيد بهذا الشرط[95].

**ب- المساعدة المتبادلة بين الدول الأطراف المتعلقة بالتدابير المؤقتة:**

وتتمثل المساعدة المتبادلة بين الدول الأطراف المتعلقة بالتدابير المؤقتة حسب هذه الاتفاقية في الحفظ العاجل للبيانات المخزنة في تقنية معلومات، والكشف العاجل للبيانات المتعلقة بتتبع المستخدمين، وهذا ما سنكتشفه في ما يلي:

**- الحفظ العاجل للبيانات المخزنة في تقنية معلومات:**

تجيز المادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لأي دولة طرف أن تقدم طلبا للحصول على الحفظ العاجل للبيانات المخزنة في تقنية المعلومات الموجودة على إقليم الدولة الطرف للطلب، على أن يشتمل هذا طلب اسمَ الهيئة المصدرة له، نوع الجريمة الإلكترونية محل التحقيق، ملخصا للوقائع، البيانات التي يتعين حفظها وبيان علاقتها بهذه الجريمة، المعلومات المتعلقة بالمسؤول عن

البيانات المخزنة وموقعها وكذا الهدف المتوخى من طلب المساعدة والذي يكون إما للوصول أو البحث أو ضبط أو كشف عن البيانات المخزنة، كما تلزم هذه الاتفاقية في المادة نفسها الدولَ الأطراف التي تتلقى طلب الحفظ العاجل للبيانات المخزنة في تقنية معلومات اتخاذ التدابير والإجراءات الضرورية لحفظ البيانات المذكورة في الطلب وفقا لقانونها الداخلي وعدم تمسكها بمبدأ ازدواجية التجريم كشرط لحفظ البيانات في الجرائم المنصوص عليها في الفصل الثاني منها، غير أنها أجازت للدول الأطراف المطلوب منها المساعدة أن ترفض هذا الطلب إذا كان تنفيذه يعرض سيادتها أو أمْنَ مصالحها الجوهرية للخطر أو إذا كانت الجريمة موضوع التحقيق تعتبر من قبيل الجرائم السياسية في قوانينها الداخلية(96).

والجدير بالملاحظة أن هذه الاتفاقية حددت المدة الدنيا للحفظ العاجل للبيانات المخزنة في تقنية معلومات المترتب على طلب المساعدة في الفقرة 07 من المادة 37 منها بستين (60) يوما، دون أن تحدد المدة القصوى لذلك.

**- الكشف العاجل لبيانات تتبع المستخدمين:**

يتعين على الدولة المتلقية لطلب المساعدة إذا ما اكتشفت، أن بيانات الحركة التي تم التطرق إليه سابقا، تفيد بأنه تمّ توجيه الإرسال من مزود خدمة في دولة ثالثة أو من الدولة الطالبة للمساعدة أن تقدم إلى هذه الأخيرة قدرا كافيا من بيانات تتبع المستخدمين لتمكينها من معرفة مزود الخدمة وتحديد مسار بث الاتصال، أما إذا كان ذلك يمس بأمنها أو سيادتها أو مصالحها أو من قبيل الجرائم السياسية فيجوز لها رفض طلب الكشف عن بيانات المستخدمين(97).

**ج- المساعدة المتبادلة للوصول إلى البيانات المخزنة واعتراض بيانات المحتوى:**

في إطار تعزيز التعاون بين الدول الأطراف في مجال مكافحة الإجرام المعلوماتي، تجيز المادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات للدول الأطراف أن تطلب من بعضها البعض القيام بأي إجراء من شأنه البحث أو النفاذ أو الضبط أو التأمين أو الكشف عن البيانات المخزنة في تقنية معلومات موجودة داخل أراضها، مع مراعاة الدول المطلوب منها المساعدة للأحكام المنصوص عليها في هذه الاتفاقية التي تنظم المساعدة القانونية المتبادلة، وكذا التزامها بالتعجيل بالرد على طلب المساعدة للدولة الطالبة في الأحوال التي تكون فيها البيانات المخزنة معرضة للحذف أو التغيير أو التعدي(98).

كما أجازت المادة 40 من هذه الاتفاقية أيضا للدول الأطراف أن تحصل على المعلومات المتوفرة للعامة في أي مكان دون حصولها على تفويض من دولة أخرى طرف، والتزامها أيضا بتقديم المساعدة لبعضها البعض بالجمع الفوري لبيانات تتبع المستخدمين التي تتم عن طريق إحدى تقنية المعلومات(99).

ونظرا لخطورة التدخل التي تتسم بها عملية الاعتراض(100)، قيدت هذه الاتفاقية على غرار اتفاقية بودابست المساعدة المتبادلة لاعتراض بيانات المحتوى في حدود ما تسمح به المعاهدات والقوانين الداخلية السارية المفعول للدول الأطراف(101).

## الخاتمـة:

نستخلص من هذه الدراسة، أن التطور العلمي في مجال تكنولوجيا المعلومات والاتصال بقدر ما كان نعمة على الإنسان حمل في طياته العديد من الآثار السلبية، كان أخطرها استغلال المنظمات الإرهابية لهذه التكنولوجيا لأغراض إرهابية متعددة.

وأن الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، وإن كانت تعتبر خطوة مهمة في تجريم الإرهاب الإلكتروني على الصعيد العربي، إلا أنها لم تجرم كل صوره في الفصل الثاني منها المتعلق بتجريم الأفعال التي ترتكب بواسطة تقنية المعلومات، وإنما جرمت فقط استعمال تقنية المعلومات لنشر أفكار التطرف وطرق صناعة المتفجرات والفتن والاعتداء على الديانات والمعتقدات، وتمويل الأعمال الإرهابية والتدريب عليها، وتسهيل الاتصال بين المنظمات الإرهابية.

غير أن هذه الاتفاقية وسعت من نطاقها في الفصل الثالث منها، المتعلق بالأحكام الإجرائية لتشمل جميع الجرائم الإلكترونية بما فيها جرائم الإرهاب الإلكتروني التي لم تنص عليها صراحة في المادة 15 منها كاختراق النظم المعلوماتية والمواقع الإلكترونية للمؤسسات والمرافق الحيوية للدول قصد تخريبها أو التجسس على المعلومات التي تحتويها أو التحكم فيها عن بعد .

ورغم تجريم هذه الاتفاقية ـ كما سبقت الإشارة إليه ـ نشر أفكار التطرف وطرق صناعة المتفجرات وإثارة الفتن والاعتداء على الديانات والمعتقدات عن طريق تقنية المعلومات، إلا أنها لم تلزم الدول الأطراف باتخاذ التدابير اللازمة لحجب المواقع الإلكترونية المتطرفة التي تزايد عددها مع تفاقم ظاهرة الإرهاب في العالم.

وقد اعتمدت هذه الاتفاقية على نوعين من الآليات لمكافحة الجرائم الإلكترونية بما في ذلك جرائم الإرهاب الإلكتروني، تتمثل الأولى في إلزامية اتخاذ الدول الأطراف للتدابير اللازمة والإجراءات الخاصة في قوانينها الداخلية لتمكين سلطاتها المختصة للبحث والتحقيق عن هذه الجرائم التي يصعب فيها التعرف على هوية المجرم، ويسهل فيها محو الدليل الرقمي، أما الثانية فتكمن في ضرورة تكثيف جهود التعاون القضائي والقانوني بين هذه الدول لعدم إفلات المجرمين من العقاب.

من خلال ما سبق ذكره، ومن أجل مكافحة جرائم الإرهاب الإلكتروني على الصعيد العربي، يمكننا تقديم الاقتراحات التالية:

- تعديل أحكام المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، لتجريم كل صور الإرهاب الإلكتروني بصريح العبارة، وتوحيد السياسة الجنائية لمنع وقمع هذه الجريمة.
- تعزيز جهود التعاون القانوني والقضائي بين الدول الأطراف لمكافحة جرائم الإرهاب الإلكتروني.
- تعزيز جهود التعاون بين الدول الأطراف لحجب المواقع الإلكترونية المتطرفة، ومراقبة نشاطاتها على شبكات التواصل الاجتماعي لقطع التواصل بين عناصرها، وسد منافذ تمويلها، والحد من تجنيد الإرهابيين عن طريق شبكة الإنترنت، مع مراعاة حق الحياة الخاصة.

- تعزيز جهود التعاون بين الدول الأطراف لتبادل الخبرات التقنية المتعلقة بالبرامج الإلكترونية الحديثة المضادة للفيروسات، والقرصنة الإلكترونية لحماية النظم المعلوماتية والمواقع الإلكترونية للمرافق الحيوية.
- تكوين كفاءات أمنية محترفة في مجال الأمن المعلوماتي للبحث والتحري عن الجرائم الإلكترونية خاصة جرائم الإرهاب الإلكتروني.
- تكثيف عمليات تحسيس وتوعية المواطن العربي، وتحذيره من أفكار التطرف التي تنشرها المنظمات الإرهابية على مواقعها الإلكترونية ومواقع التواصل الاجتماعي.
- تنظيم ملتقيات دولية وندوات علمية حول مخاطر الإرهاب الإلكتروني على أمن الدول العربية ومصالحها السياسية والاقتصادية.

## الهوامش:

(1) جمال زايدان هلال أبو عين، الإرهاب وأحكام القانون الدولي، عالم الكتاب الحديث للنشر والتوزيع، بدون طبعة، 2008، ص 19.

(2) نادية شرايرية، إشكالية تعريف الإرهاب في القانون الدولي، مجلة التواصل في العلوم الإنسانية والاجتماعية، جامعة باجي مختار – عنابة (الجزائر) المجلد 19، العدد 02، 2013، ص 154.

(3) هيثم عبد سلام محمد، مفهوم الإرهاب في الشريعة الإسلامية، دار الكتب العلمية، بيروت، الطبعة الأولى، 2005، ص 23.

(4) أسامة حسين محي الدين، جرائم الإرهاب على المستوى الدولي، المكتب العربي الحديث، الإسكندرية، بدون طبعة، 2009، ص 57.

(5) GHANEM-LARSON Abir, essai sur la notion d'acte terroriste en droit international pénal, thèse de doctorat en droit international public, université d'Aix-Marseille-III, 2010/2011, p 35.

(6) يوسف كوران، جريمة الإرهاب والمسؤولية المترتبة عنها في القانون الجنائي الداخلي والدولي، مركز كردستان للدراسات الاستراتيجية، السليمانية، بدون طبعة، سنة 2007، ص 12.

(7) عثمان علي الحسن ويسي، الإرهاب الدولي ومظاهره القانونية والسياسية في ضوء أحكام القانون الدولي العام، دار الكتب القانونية، مصر، بدون طبعة، 2011 ص 65.

(8) للاطلاع على قرار الجمعية العام للأمم المتحدة رقم 3034 المؤرخ في 18 ديسمبر 1972، المتعلق بالتأكيد على قانونية النضال من أجل التحرر الوطني وإقامة لجنة خاصة لدراسة مشكلة الإرهاب الدولي، انظر الرابط الإلكتروني:
http://www.moqatel.com/openshare/Wthaek/UNDocs/GmeiaAmah/index2.htm، تاريخ الاطلاع: 2017/10/25.

(9) مصطفى مصباح دباره، الإرهاب مفهومه وأهم جرائمه في القانون الدولي الجنائي، منشورات جامعة قاريونس، بنغازي، الطبعة الأولى، 1990، ص 117.

(10) إمام حسانين عطا الله، الإرهاب والبنيان القانوني للجريمة دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية، بدون طبعة، 2005، ص 104.

(11) سامي علي حامد عياد، تمويل الإرهاب، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2008، ص 26.

(12) عبد الله نور شعت، التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2017، ص 51.

(13) منتصر سعيد حمودة، الإرهاب الدولي جوانبه القانونية ووسائل مكافحته في القانون الدولي العام والفقه الإسلامي، دار الفكر الجامعي، الإسكندرية، الطبعة الأولى، 2008، ص 38.

(14) حسنين المحمدي بوادى، حقوق الإنسان بين مطرقة الإرهاب وسندان الغرب، دار الفكر الجامعي، الإسكندرية، بدون طبعة، 2006، ص 59.

(15) مسعد عبد الرحمان زيدان، الإرهاب في ضوء أحكام القانون الدولي العام، دار الكتب القانونية، مصر، بدون طبعة، 2005، ص 65.

(16) بوازدية جمال، الاستراتيجيات المغاربية لمكافحة الإرهاب، أطروحة دكتوراه في قسم الدراسات الدولية، جامعة الجزائر3، 2013/2012، ص 40.

(17) محمد فتحي عيد، واقع الإرهاب في الوطن العربي، أكاديمية نايف للعلوم الأمنية، الرياض، بدون طبعة، 1999، ص 24.

(18) محمد محيي الدين عوض، تعريف الإرهاب، مداخلة مقدمة للندوة العلمية الموسومة بعنوان "تشريعات مكافحة الإرهاب في الوطن العربي"، المنظمة من طرف جامعة نايف للعلوم الأمنية بالسودان، خلال الفترة من 07 إلى 09 ديسمبر 1998، من ص 52 إلى ص 53، على الرابط الإلكتروني: http://www.nauss.edu.sa/Ar/DigitalLibrary/Books/Pages/CrimeinArab.aspx?BookId=439، تاريخ الاطلاع: 2017/11/13.

(19) http://www.larousse.fr/dictionnaires/francais/cyberterrorisme/186900, consulté le **13**/**11**/2017**.**

(20) http://dictionnaire.cordial-enligne.fr/definition/cyberterrorisme, consulté le **13**/**11**/2017.

(21) قراصنة المعلومات: هم "الشباب البالغ المفتون بالمعلوماتية والحاسب الآلي الذين لديهم قدرة فائقة على اختراق الشبكات والإبحار في عالم البيانات، دون أهمية لحواجز كلمات المرور أو السر أو الشفيرات، ولكن أهم ما يميز هذه الطائفة عدم وجود نية أو قصد لإتلاف المعلومات أو تخريب أنظمة الحاسب وشبكات الاتصال، ولكن هدفهم هو الاستكشاف في العالم الخيالي، والميل إلى المغامرة والتحدي. ونادرا ما تكون أفعالهم المحضورة غير شريفة". نقلا عن: ياسمينة بونعارة، الجريمة الإلكترونية، مجلة المعيار، كلية أصول الدين، جامعة الأمير عبد القادر للعلوم الإسلامية - قسنطينة (الجزائر)، المجلد 20، العدد 39، 2015، ص 284.

(22) DESFORGES ALIX, cyber terrorisme: quel périmètre, fiche n° 11 de l'institut de recherche stratégique de l'école militaire (IRSEM), décembre 2011, sur le site web :
http://www.defense.gouv.fr/irsem/publications/archives/fiches/fiches-de-l-irsem, consulté le **15/11/2017**.

(23) http://www.talabanews.net, consulté le **15/11/2017**.

(24) PAGET François, l'hacktivisme, article publié sur le site web:
http://www.chaire-cyber.fr/IMG/pdf/article_2_3_-_chaire_cyberdefense_2_.pdf, consulté le **17/11/2017**.

(25) أحمد فلاح العموش، مستقبل الإرهاب في هذا القرن، جامعة نايف للعلوم الأمنية، الرياض، بدون طبعة، 2006، ص 90.

(26) أمير فرج يوسف، الجريمة الإلكترونية والمعلوماتية والجهود الدولية والمحلية لمكافحة جرائم الكمبيوتر والإنترنت، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2011، ص 219.

(27) عبد المجيد الحلاوي، أهمية التعاون الدولي والعربي في مكافحة جرائم الإرهاب المعلوماتي، مداخلة مقدمة للدورة التدريبية الموسومة بمكافحة الجرائم المعلوماتية الإرهابية، المنظمة من طرف جامعة نايف للعلوم الأمنية بالقنيطرة (المغرب)، خلال الفترة من 09 إلى 13 أفريل 2006، ص 08، على الرابط الإلكتروني: http://www.nauss.edu.sa، تاريخ الاطلاع: 2017/11/25.

(28) http://democraticac.de/?p=34528, consulté le **25/11/2017**.

(29) رائد العدوان، المعالجة الدولية لقضايا الإرهاب الإلكتروني، مداخلة مقدمة للدورة التدريبية الموسومة بتوظيف شبكات التواصل الاجتماعي لمكافحة الإرهاب، المنظمة من طرف جامعة نايف للعلوم الأمنية بمدينة الرياض، خلال الفترة من 23 إلى 27 فيفري 2013، ص 08، على الرابط الإلكتروني: http://www.assakina.com/book/73801.html، تاريخ الاطلاع: 2017/11/26.

(30) المرجع نفسه، ص 08.

(31) http://democraticac.de/?p=34528, consulté le **29**/**11**/2017.

(32) مصطفى يوسف كافي، جرائم "الفساد، غسيل الأموال، السياحة، الإرهاب الالكتروني، المعلوماتية"، مكتبة المجتمع العربي للنشر والتوزيع، الطبعة الأولى، 2014، من ص 143 إلى ص 144.

(33) يوسف حسن يوسف، الجرائم الدولية للإنترنت، المركز القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، 2011، من ص 135 إلى ص 136.

(34) أمير فرج يوسف، مرجع سابق، ص 219.

(35) غزيل عائشة، ماهية الجريمة المعلوماتية، مداخلة مقدمة للملتقى الوطني حول "الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري"، المنظم بالمركز الجامعي لغليزان، خلال الفترة من **07** إلى **08** فيفري 2017، ص 07.

(36) فايز بن عبدالله الشهري، ثقافة التطرف والعنف على شبكة الإنترنت: الملامح والاتجاهات، مداخلة مقدمة للندوة العلمية "استعمال الإنترنت في تمويل الإرهاب وتجنيد الإرهابيين"، المنعقدة بمدينة القاهرة، خلال الفترة من 25 إلى 27 أكتوبر 2010، ص 09، على الرابط الإلكتروني: https://repository.nauss.edu.sa/discover ، تاريخ الاطلاع: 2017/12/02.

(37) http://www.ce4arab.com/vb7/showthread.php?t=597540, consulté le **05/12**/2017.

(38) يوسف حسن يوسف، مرجع سابق، من ص 104 إلى ص 106.

(39) ليتيم فتيحة، ليتيم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة المفكر، كلية الحقوق والعلوم السياسية، جامعة محمد خيضر - بسكرة (الجزائر)، العدد 12، 2015، ص 246.

(40) بن طيفور نسيمة، الفيروسات وجرائم النظم المعلوماتية، مداخلة مقدمة للملتقى الوطني حول " الإطار القانوني لاستخدام تقنية المعلومات في التشريع الجزائري"، المنظم بالمركز الجامعي لغليزان خلال الفترة من **07** إلى **08** فيفري 2017، ص 04.

(41) رامي حليم، جرائم الاعتداء على أنظمة المعالجة الآلية للمعلومات، مجلة دراسات وأبحاث، جامعة زيان عاشور- الجلفة (الجزائر)، المجلد 01، العدد 01، 2009، ص 349.

(42) يوسف حسن يوسف، مرجع سابق، ص 109.

(43) http://www.vetogate.com/1346396, consulté le **08/12/2017**.

(44) تنص المادة 15 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010، على أن "الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات:

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها؛

**2**- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية؛

**3**- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية؛

**4**- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات".

(45) عبد العال الديربي، محمد صادق إسماعيل، الجرائم الإلكترونية "دراسة قانونية قضائية مقارنة مع أحدث التشريعات العربية في مجال مكافحة جرائم المعلوماتية والإنترنت"، المصدر القومي للإصدارات القانونية، القاهرة، الطبعة الأولى، 2012، من ص 270 إلى ص 271.

(46) مشبب ناصر محمد آل زبران، المواقع الإلكترونية ودورها في نشر الغلو الديني وطرق مواجهتها من وجهة نظر المختصين، ماجستير في العلوم الإدارية، جامعة نايف للعلوم الأمنية، 2011/2010، ص 11.

(47) http://www.journaldunet.com, consulté le **14/12/2017**.

(48) http://baathparty.sy/site/arabic/index.php?node=552&cat=15369&, consulté le **14/12/2017**.

(49) تعرف شبكات التواصل الاجتماعي بأنها "منظومة الشبكات الإلكترونية التي تسمح للمشترك فيها بإنشاء موقع خاص به، ومن ثمة ربطه من خلال نظام اجتماعي إلكتروني مع أعضاء آخرين لديهم نفس الاهتمامات والميول، أو جمعه مع أصدقائه". نقلا عن فهد علي الطيار، شبكات التواصل الاجتماعي وأثرها على القيم لدى طلاب الجامعة "توتير نموذجا" دراسة تطبيقية على طلاب جامعة الملك سعود، المجلة العربية للدراسات الأمنية والتدريب الرياض (السعودية)، المجلد 31، العدد 61، ص 202.

(50) http://www.al-jazirah.com/2016/20161208/pl1.htm, consulté le **17/12/2017**.

(51) https://weedoo.tech/**2017**, consulté le **17/12/2017**.

(52) http://www.assakina.com/files/books/book8.pdf, consulté le **18/17/2017**.

(53) http://www.masralarabia.com, consulté le **18/12/2017**.

(54) https://www.sasapost.com, consulté le **23/12/2017**.

(55) محمد السيد عرفة، تجفيف مصادر تمويل الإرهاب، جامعة نايف للعلوم الأمنية، الرياض، الطبعة الأولى، 2009، ص 22.

(56) انظر المادة 01/ف01 من الاتفاقية العربية لمكافحة غسيل الأموال وتمويل الإرهاب لعام 2010.

(57) http://hackandspamdz.blogspot.com/2014/09/blog-post.html, consulté le 23/12/2017.

(58) انظر المادة 02/ف3 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(59) انظر المادة 01/ف4 من نظام مكافحة الجرائم المعلوماتية بالمملكة العربية السعودية، الصادر بموجب المرسوم الملكي رقم م/17 المؤرخ في 08/03/ 1428 هـ.

(60) بوعنادة فاطمة الزهرة، مكافحة الجريمة الإلكترونية في التشريع الجزائري، مجلة الندوة للدراسات القانونية، العدد الأول، 2013، ص 71، على الرابط الإلكتروني: **https://revuena**dwa.jimdo.com، تاريخ الاطلاع: 2017/12/26.

(61) انظر التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية، الصادر بتاريخ 2001/11/08، على الرابط الإلكتروني:

https://rm.coe.int/explanatory-report-budapest-convention-in-arabic/1680739174، تاريخ الاطلاع: 2017/12/26.

(62) انظر المادة 23 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(63) انظر المادة 25 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(64) انظر المادة 01 من اتفاقية بودابست المتعلقة بالجرائم المعلوماتية لسنة 2001، على الرابط الإلكتروني:
http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_fr.pdf
تاريخ الاطلاع: 2018/01/03.

(65) أحمد مسعود مريم، آليات مكافحة القانون الجرائم المتصلة بتكنولوجيا الإعلام والاتصال في ضوء القانون رقم 04/09، رسالة ماجستير في القانون الجنائي، جامعة قاصدي مرباح _ ورقلة، 2013/2013، ص 97.

(66) انظر المادة 26 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(67) انظر المادة 05 من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47، الصادر في 2009/08/16.

(68) انظر المادة 47/ف03 من قانون الإجراءات الجزائية الجزائري.

(69) أحمد مسعود مريم، مرجع سابق، ص 94.

(70) http://www.th3professional.com/2010/11/blog-post_5845.html , consulté le 08/01/2018.

(71) انظر المادة 27 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(72) انظر المادة 28 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(73) محمد الطاهر، التعليق على الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، على الرابط الإلكتروني: **https://afteegypt.**org/digital_freedoms/2015/03/11/9770-afteegypt.html، تاريخ الاطلاع: 2017/01/10.

(74) انظر التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية، مرجع سابق.

(75) المرجع نفسه.

(76) انظر المادة 03 من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47، الصادر في 2009/08/16.

(77) انظر المادة 03 من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47، الصادر في 2009/08/16.

(78) انظر المادة 04/ف3 من القانون رقم 04/09 المؤرخ في 05 أوت 2009، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال، الجريدة الرسمية، العدد 47، الصادر في 2009/08/16.

(79) إمام حسنين خليل، التعاون القضائي الدولي لمواجهة الجريمة المنظمة دراسة مقارنة بين الاتفاقية الدولية لمكافحة الجريمة المنظمة عبر الوطنية والقانون الإماراتي، ص 05، مقال منشور في شهر جانفي 2015، تاريخ الاطلاع: 2018/01/14، الرابط الإلكتروني للمقال:
http://strategicvisions.ecssr.com/ECSSR/ECSSR_DOCDATA_PRO_EN/Resources/PDF/Rua_Strategia/Rua-Issue-09/rua09_08.pdf

(80) عبد الله نور شعت، التعاون الدولي في مكافحة الجريمة المنظمة والإرهاب الدولي، مكتبة الوفاء القانونية، الإسكندرية، الطبعة الأولى، 2017، ص 308.

(81) انظر المادة 102 من نظام روما الأساسي للمحكمة الجنائية الدولة لسنة 1998، الذي دخل حيز النفاذ في 2002/07/01، على الرابط الإلكتروني: http://legal.un.org/icc/statute/arabic/rome_statute(a).pdf، تاريخ الاطلاع: 2018/01/17.

(82) انظر المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(83) انظر المادة 34/ف1 و2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(84) انظر المادة 34/ ف8 "أ"- "ب"-"ج" من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(85) انظر المادة 31 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

**(86)** http://elibrary.mediu.edu.my/books/MAL03126.pdf, consulté le **18/01/2018**.

(87) فريد بايبر وشون ميرفي، ترجمة محمد سعد طنطاوي، علم التشفير، مؤسسة هنداوي للتعليم والثقافة، القاهرة، الطبعة الأولى، 2016، ص 15.

(88) http://infdatint.blogspot.com/2015/03/blog-post_23.html, consulté le **18/01/2018**.

(89) انظر المادة 32/ف4 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(90) انظر المادة 35 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(91) انظر المادة 34/ف4، 5، 6 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(92) انظر المادة 36 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(93) انظر المادة 33/ف1 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(94) انظر التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية، مرجع سابق.

(95) انظر المادة 33/ف2 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(96) انظر المادة 37 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(97) انظر المادة 38 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(98) انظر المادة 39 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(99) انظر المادة 41 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.

(100) انظر التقرير التفسيري لاتفاقية بودابست للجريمة الإلكترونية، مرجع سابق.

(101) انظر المادة 42 من الاتفاقية العربية لمكافحة جرائم تقنية المعلومات لعام 2010.